UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/237,016	01/25/1999	LA VAUGHN F. WATTS JR.	M-6084US	9706

23640 7590 03/22/2004

BAKER BOTTS, LLP
910 LOUISIANA
HOUSTON, TX 77002-4995

EXAMINER	
JACKSON, JENISE E	

ART UNIT	PAPER NUMBER
2131	17

DATE MAILED: 03/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/237,016	WATTS ET AL.	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,9-38 and 40-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,9-38 and 40-42* is/are rejected.

7)☒ Claim(s) *7 and 8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo and (Authoritative Dictionary of IEEE Standards) and further in view of Lambert.

5. As per claim 1, Angelo discloses a computer system(see fig. 1, sheet 1, and col. 4, lines 39-40), a processor(102)(see fig. 1, sheet 1, and col. 4, lines 49-50), an access token communicator(i.e. probe) for reading a token(i.e. smartcard)(see col. 6, lines 13-15, 33-36), an input device(158) of being capable of being coupled to the processor(see fig. 1, sheet 1), the input device being adapted to receive a security code(i.e. pin/plain text password)(see col. 3, lines 40-41). The Examiner asserts that comparing the password to verification data on the access token, is inherent, because Angelo discloses that a password is entered once the token is inserted (see col. 3, lines 40-48). Thus, if the two passwords match(i.e. verification data), than this confirms that the user is authorized to use the access token(see col. 3, lines 46-48).

6. According to the Authoritative Dictionary of IEEE Standards, security level is defined as a hierarchical level whose purpose is to indicate degree of sensitivity to a designated security threat. It indicates a specific level of protection as specified by the security policy being enforced(see pg. 1015). Thus, since Angelo discloses security levels than Angelo discloses a security policy. Angelo discloses security policies(i.e. security levels) that can require different levels of access to different resources by having different passwords(see col. 13, lines 19-22),

thus access to the resources will be based on what password the user has been granted. Furthermore, Angelo discloses a software system executable on the processor, and including a system security process controlling operational access to the processor, because Angelo discloses that an access token communicator for reading data on the token and comparing the data that is inputted with data stored on the token. Thus, the comparison of the data, contains software inherent in order to verify the user to a particular resource. Also, Angelo discloses an access token and verification data(see col. 3, lines 33-38), setting security policies(i.e. levels), and controlling access to resources based on the security policies(i.e. levels)(see col. 13, lines 18-22).

7. The Examiner takes Official Notice that it is well-known in the art to have a software system that contains executable program code, the motivation is that the executable program code is a complied program translated into machine code in a format that can be loaded into memory and run by a computer's processor. Thus, the motivation of having executable program code is that it allows the software to run.

8. Angelo does not disclose a receiving a set of security policies from the access token in the processor in response to verification data. Lambert discloses in response to verification data, a set of security policies(i.e. levels) are received(see col. 2, lines 29-36, and col. 2, lines 4-16). Further, Lambert controls access to resources based on security policies(i.e. levels)(see col. 2, lines 43-44).

9. Both (Angelo and IEEE Standards) with Lambert disclose access control with smartcard. It would have been obvious to include the feature of Lambert that discloses in response to verification data, a set of security policies are received, with Angelo and IEEE standards. The motivation is that Lambert recognizes a problem when seeking to control access to application

program modules where a number of different users are required to be allowed access different security modules(see col. 1, lines 48-51 of Lambert). Lambert also discloses the conventional approach is that a table lookup process scans a static list to determine the access authority of the user, and the user is given access to certain applications according to their determined authority level(see col. 1, lines 55-61 of Lambert). Thus, such conventional system relying on lookup tables of user authorities are vulnerable to breaches of security even if the applications themselves are held in protected form(see col. 1, lines 62-65 of Lambert). An unauthorized person may seek to add themselves to the list or to change their authority level within the list(see col. 1, lines 65-67 of Lambert). Therefore, Lambert provides a more protective measure of providing access to users by storing the access level on the card in the form of a key or dynamically generating the security policy once the user has typed in his/her PIN(see col. 2, lines 29-36).

10. Rejected under same basis as claim 1 and further, As per claim 2, Angelo discloses a non-volatile storage device operably coupled to the processor(see fig. 1, sheet 1), and a non-volatile storage device(see col. 5, lines 57-60) access password that selectively allows access to the nonvolatile storage device, wherein the nonvolatile storage device password is supplied in response to the access token reading device reading an access token and the input device receiving valid verification data(see col. 7, lines 54-58, col. 8, lines 19-25, 37-40).

11. As per claim 3, Angelo discloses at least one of a set of policies(i.e. security levels) is stored within the nonvolatile storage device password(see col. 13, lines 12-14, 19-25, 34-43).

12. As per claim 4, Angelo discloses wherein at least one of the set of policies (i.e. levels) is stored on the access token, because Angelo discloses that the user can have varying levels of

access based on the password, thus when the user enters the password, this password is encrypted and compared to a encrypted value stored on the card (see col. 13, lines 19-24, 29-40).

13. As per claim 5, Angelo discloses that one of the one or more policies (i.e. levels corresponds to the verification data, because Angelo discloses that when the user enters different passwords that are associated with different levels (i.e. policies) of access to the computer system, and if the user's password matches the password stored on the token (i.e. verification data), than the user is allowed access to certain resources based on the password that the user receives (see col. 13, lines 19-23, 30-43).

14. As per claim 6, limitations have already been addressed see claim 1 and 15, further, the Examiner takes Official Notice that by having a security policy for bios control information is well-known, the motivation is that the user can change system settings and other configuration information dealing with the system.

15. As per claim 9, Angelo discloses a password corresponding to the nonvolatile storage device access password (i.e. peripheral password) is stored on the access token (see col. 3, lines 41-44).

16. As per claims 10-11, Angelo discloses that the access token (i.e. smartcard) includes one or more bytes of data in a non-keyboard enterable format (i.e. biometrics)(see col. 7, lines 47-53).

17. As per claim 12, Angelo discloses wherein the verification data (i.e. password entered by way of biometrics) includes biometric data supplied by a user (see col. 7, lines 47-53).

18. As per claim 13, Angelo discloses that the input device includes a keyboard for entering in the password, and the verification data includes a password (i.e. PIN) stored on the card (see col. 3, lines 40-48).

19. As per claim 14 rejected under the same basis as claims 1-2, except, Angelo discloses one or more policies (i.e. levels) associated with the operating system, and wherein the operating system includes security code selectively enabled by the one or more policies to limit access to the computer system responsively to an access token read by the access token communication device (see col. 7, lines 15-25, 43-50, and col. 13, lines 18-25), and the access token communication device (i.e. computer) is the computer in Angelo because Angelo discloses that the computer is able to detect the presence of the token that is coupled to the computer(see col. 3, lines 33-39), the input device operable to transmit a security code(i.e. password) from a user to one or more processors(see col. 3, lines 52-54), the operating system inherent, permitting access to the nonvolatile storage device and the one or more processors if the security code and the set of security policies(i.e. levels) match an authorization data stored in nonvolatile memory(see col. 9, lines 12-29, 54-56, col. 13, lines 8-27).

Claims 15-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lambert and (Authoritative Dictionary of IEEE Standards) and further in view of Angelo.

20. As per claim 15, limitations have already been addressed see claim 1. Further, limitations of claim 15, Lambert discloses a set of security policies associated with the operating system, the operating system operable to receive the security code for selectively enabling the security policies to limit access to the computer system(see col. 2, lines 32-50). Lambert fails to disclose operating system permitting access to the non-volatile storage device and one or more

processors if the security code match an authorization data stored in nonvolatile memory; however, Angelo teaches that the security code(i.e. peripheral password) matches the authorization data stored in non-volatile memory(see col. 3, lines 44-46). It would have been obvious to combine Lambert with Angelo, to include the features of security policies(i.e. level), the motivation is that Lambert teaches that in prior art a lookup table process scans a static list to determine access authority of the user and the require security level(see col. 1, lines 58-61), and further teaches that such conventional systems relying on lookup tables of user authorities are vulnerable to breaches of security(see col. 62-65).

21. As per claim 16, Angelo discloses wherein the operating system includes a BIOS and wherein the BIOS is stored on nonvolatile memory that is electrically interconnected to the one or more processors (see col. 7, lines 15-22, fig. 1, sheet 1).

22. As per claim 17, Angelo discloses the access token communication device includes a smart card communication device (see col. 6, lines 13-22, 33-36).

23. As per claim 18, Angelo discloses the access token communication device includes network circuitry (i.e. adapted to receive signals) from one or more computers interconnected on a computer network (col. 5, lines 17-20, 51-53).

24. As per claim 19, Angelo discloses the access token communication device includes a modem that receives signals from a communication line.

25. As per claim 20, wherein the input device is a keyboard (159)(see fig. 1, sheet 1, col. 9, lines 49-50)

26. As per claim 21, Although Angelo does not expressly disclose a biometric reading device; Angelo does disclose that the user can input information by using a biometric device (see

col. 7, lines 50-53). The Examiner takes Official Notice that a biometric reading device is well-known, thus it would be obvious to have a biometric reader, because the motivation is that a biometric reader allows one to read the biometric data input by the user.

27. As per claims 22-23, Although Angelo discloses a fingerprint scanner; a retinal scanning device(i.e. biometrics)(see col. 7, lines 50-53).

28. As per claim 24, Angelo discloses the nonvolatile storage device includes a hard disk drive(see col. 5, lines 56-59).

29. As per claim 25, Angelo discloses a data access code stored in the nonvolatile memory, wherein a data request code corresponding to the data access code alters a state of the nonvolatile storage device, because Angelo discloses that if the data request code corresponds to the data access code(i.e. peripheral password stored in storage), than the state is altered by unlocking the storage device from locked to unlocked(see col. 9, lines 32-38, 43-48).

Claims 26-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo (Authoritative Dictionary of IEEE Standards), Lambert, and further in view of Avarne.

30. As per claim 26, limitations have already been addressed see claim 1 and 15. Further, claim 26 rejected by Angelo for a nonvolatile storage device access password that selectively allows access to the nonvolatile storage device, wherein the nonvolatile storage device password is supplied in response to the access token reading device reading an access token and the input device receiving verification data. Angelo does not disclose a master password. However, Avarne discloses a master password(see col. 3, lines 24-42).

It would have been obvious to combine Angelo with Avarne, the motivation to include a master password is that a master password allows unlocking an inadvertently locked token(see

col. 1, lines 37-40 of Avarne). Therefore, the motivation to have a master password is that the master password seeks to provide a means for the unlocking of locked token which can avoid the need to return such tokens to their issuing authority while at the same time avoiding the possible dissemination of information useful for subverting their locking function(see col. 1, lines 52-57).

31. As per claim 27-34 limitations have already been addressed see claims 1 and 15.

32. As per claim 35, Angelo discloses that transferring one or more passwords from the access token to a computer system, because once the user enters the password, and the password is encrypted to produce a peripheral password, and this password is a system password that is combined with the password stored in memory (see col. 9, lines 33-35, 43-48).

33. As per claim 36, Angelo discloses transferring is in response to an access code received by the access token, because Angelo discloses that the access code(i.e. password) is inputted by the user(see col. 3, lines 40-41), and then transferred to the computer system(see col. 3, lines 44-48).

34. As per claims 37-38, Angelo discloses wherein one of the one or more passwords corresponds to a computer system password installed on the computer system(see col. 8, lines 20-23), and wherein one of the one or more passwords corresponds to a nonvolatile storage device password installed on a nonvolatile storage device(see col. 9, lines 12-32).

35. As per claim 40, Angelo discloses wherein the one or more security policies(i.e. levels) are stored in an encrypted format, because based on the password that the user has entered is encrypted and this encrypted key has policies that are associated that allow a user to access certain resources or devices(see col. 3, lines 37-48, and col. 13, lines 18-26). Further, Microsoft

Computer Dictionary defines a data stream to be a byte-by-byte flow of data(see pg. 110). Therefore, a data stream(i.e. password) is bytes of data.

36. As per claims 41-42, recited the same limitations as claim 14, and further means for reading an access token, means for receiving an authentication password(i.e. peripheral password), means for verifying the validity of the access token based on the authentication password, means for unlocking a nonvolatile storage device on the computer(see col. 9, lines 13-38, 43-54). As per the limitation of security policies has already been addressed see claim 1 above.

37. As per claims 7-8 are indicated as being objected to because rejected under base claims. The limitations of wherein one of the one or more polices includes a BIOS control information that is used to configure the computer system, wherein the BIOS control information further includes password change information, the password change information including one or more password change settings for a user using the one or more security policies. Prior art such as Angelo and Lambert fails to disclose these limitations although both disclose security policies neither Angelo nor Lamber discuss what type of policies that will give the user access to a particular type of service or resource.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached on (703) 305-9711. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-0040 for regular communications and (703) 308-6306 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

***

November 2, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100